Applied Research Frontiers

Ariviyal Publishing

Research Article

DOI: 10.36686/Ariviyal.ARF.2022.01.03.016

Appl. Res. Front., 2022, 1(3), 22-25.

Students' Cybersecurity Awareness at Yemenis Educational Institutions

Abdullah Rashed,* Fua'ad Abdulrazzek and Saida Kurkshy

Yemen Center for Information Technology in Higher Education, Sana'a, Yemen.

***Corresponding author E-mail address**: abdullah.rashed@gmail.com (Abdullah Rashed)

ISSN: 2583-3065

Crossref

Abstract: This study aims to explore the level of cybersecurity awareness among students at education institutions in Yemen. Descriptive methodology was followed. A questionnaire tested students in terms of four variables: cybersecurity knowledge; self-perception of cybersecurity skills, actual cybersecurity skills and behavior; and cybersecurity attitudes. The responses revealed several misalignments which make the students potentially vulnerable to cyber-attacks. The findings demonstrate the need to target cybersecurity awareness campaigns that address the specific weaknesses of particular populations of users.

Keywords: Yemen cybersecurity; awareness; student awareness

Publication details
Received: 16th November 2022
Revised: 21st December 2022
Accepted: 21st December 2022
Published: 30th December 2022

1. Introduction

An internet interconnection grows exponentially.[1-8] This growth is accompanied by significant growth of cyber-attack incidents.[6,9] A large percentage of internet users are unaware of cybersecurity policies and practices.[1] Studies indicated that the students claimed to have basic cybersecurity knowledge, but are not aware of how to protect their data.[7] In addition, youths are easy targets to cybersecurity threats as they surf many social and gaming sites.[9]

Moreover, most universities do not have an active cybersecurity awareness program to improve students' knowledge on how to protect themselves from any threats.[6]

Cybersecurity is focused on helping the community to make knowledgeable decisions on its adaptation and mitigation.[12] Importance of cybersecurity is increasing due to the rise of reliance on digital equipment and programs to manage our daily lives, including the transmission and storage of personal information.[11] Cybersecurity has been an essential prerequisite for almost every organization to handle the massive number of emerging cyber-attacks worldwide.[5]

Thus, Cybercrimes have accelerated fast over the past decade.[14] The worst is that it's expected that it would increase.[4] As a reaction, cybersecurity is growing exponentially in both the public and private sectors.[6] Moreover, the growing rate of cybercrime makes users more deal with it as a danger.[1]

However, cyberattacks are difficult to track as attackers know how to escape from being tracked or identified due to the anonymous nature of the internet. Cybercriminals do not have to use a lot of money for their cyberattacks as the Internet is more convenient and cheaper than physical attacks.[9]

A critical factor in reducing the possibility of being harmed is cybersecurity awareness. Security awareness plays a pivotal role in our daily life nowadays. The worst is that it is expected that the number of cyber-attacks will grow shortly. That makes it urgent to developing a defensive strategy needs a comprehensive study.[5] As cybersecurity awareness (CSA) is a key defense in the protection of people and systems.[4] The lowest level in the developing country is to use university program in cybersecurity awareness to mitigate cyberattacks.[6]

Most studies have indicated the lack of proper cybersecurity awareness and a need awareness program is needed to increase the level of awareness and minimize successful cyber-attacks.[7]

Similar researches were conducted in different countries to see the level of cybersecurity in Nigeria, Bangladesh, the US, Nigeria, South Africa, Pakistan, Srilanka and Saudi Arabia.

The literature calls for initiating cybersecurity awareness programs in addition to training and education.

Table 1. Sample education

Variable		No. of participants	SMA
Qualification	Bachelor	94	82%
	Diploma	3	3%
	M.A (Master)	11	10%
	PhD	6	5%
Experience	Less than 5	97	85%
	5-10	4	4%
	More than 10	9	8%
	Missed	4	4%
Training on Cyber Security	Trained	3	3%
	Did not train	108	95%
	Missed	3	3%

2. Literature review

Butler et.al (2014), Pramod et.al (2014) and Aljohani et.al (2020), etc. found that users have good level of awareness. In contrast, Butler et.al., (2014) found that users consider suitability a priority element over security as only 23% of users change their passwords daily whereas 70% of users representing that it is good practice.[3]

Pramod et.al, (2014) found that higher education students are aware of security concerning smartphones, but they are not fully aware of the security risks and their practices.

Kim (2014) found that the US University students' needed to participate more in cybersecurity awareness programs to be well aware of information security issues.

Nagahawatta et.al, (2018) evaluated the level of cybersecurity awareness amongst university students in Sri Lanka. They found that university students in Sri Lanka were able to identify cybercrime as a threat. Thus, they ranked cybersecurity awareness and experiences among university students in Sri Lanka are not significantly low. However, reported that university students have some knowledge gaps with new threats. They recommended paying attention to the necessitate of building awareness and developing the capacity to improve student's knowledge on the cybersecurity subject especially if universities are to be used as a key focal point in cybersecurity awareness campaigns in Sri Lanka.

Irfan et.al. (2020) investigated the awareness of cybersecurity among university students who belong to different domains in Pakistan. They found that cybersecurity awareness programs should be organized.

Aljohani et.al, (2020) found that the students' awareness is at an average level. No gender difference in cybersecurity awareness, or student's class level. They recommended necessary policy measures to be taken to ensure that students from all batches have the same level of cybersecurity awareness.

Elradi et.al, (2020) studied three security elements: trust, passwords, and defensive attitude. They found that all participants were having a fairly low level of security awareness and their defensive attitude to be weak and don't protect them either individually or at the institutional level.

They recommended using to develop training approaches that bridge the security gaps.

Garba et.al, (2020) found that there is not any approach in place to increase the level of cybersecurity awareness to students at universities in Nigeria. The results also show that students lack the basic knowledge of cybersecurity.

Chandarman (2017) found users vulnerable. Literature in general suggests presenting solutions as curriculum, training courses and awareness.

Hariri et.al, (2020) investigated the level of cybersecurity awareness among female teachers. They found the sample in the middle level. Thus, they recommended organizing security courses and workshops to aware society. Tibi et.al. (2019) studied the computer science Arab student's cybercrime awareness. They found that higher education institutions have to build awareness programs that provide training courses on cybersecurity to all students.

Kurt et.al, (2016) developed a module that raises cybersecurity awareness. They found their module useful to understand the level of awareness and raises cybersecurity awareness level. Moreover, they found non-Computer Science (CS) majors to be affected and their level of awareness raised overall in cybersecurity.

Ahmed et.al, (2019) recommended developing and implementing a cybersecurity awareness program as an urgent requirement to immune the citizens from cyber threats. Furthermore, they suggested that government need to work together with public and private sectors, the academia in creating cyber awareness among everyone to make the best for a country, to make Bangladesh more cyber robust.

Generally, the literature is that training and education are key initiatives to create cybersecurity awareness.

The literature suggests that cybersecurity awareness elements for assessment are knowledge, self-perception of skills, actual skills and behaviors, and attitudes.[7]

3. Methodology

The purpose of this study is to examine the cybersecurity awareness levels of individuals currently enrolled in higher education; particularly those individuals who among youths in the area of Information Systems (IS) at the bachelor's level. This is in response to the general belief that such backgrounds of study are conducive to higher and/or similar awareness levels of security issues in cyberspace, since exposure to IT.

3.1. Research Hypothesis

This study is limited to the academic environment of groups of students currently enrolled in a bachelor's degree program in Information Systems and/or Information Technology. Further, it is a general belief that individuals enrolled in higher education in such fields of study are more exposed to current information regarding cybersecurity (i.e. information and data security, cyber-threats, best practices, standards, etc.) and that they remain informed about the latest cybersecurity issues by exposure and/through individual interactions in academic settings.

The hypotheses seek to examine relationships, if any, between cybersecurity awareness level and the background of the participants, focusing specifically on three demographic variables: 1) Academic qualification; 2) Years of experience (using the Internet); 3) Cybersecurity training.

Table 2. Questions

S.No	Research Questions	Agree strongly	Agreed	Neutrals	Not agree	Not strongly agree
1	I support the university's request to change the password periodically	53	24	15	11	8
2	I back up my files to an external memory	65	32	5	4	5
3	Use spyware protection files	69	20	15	4	3
4	I keep my files and photos in more than one place to avoid theft or damage	66	23	8	12	2
5	Beware of sharing my personal information with strangers on the	90	11	7	2	1
6	Check the sources of information circulating on social media before sending it to others	83	14	9	4	1
7	Respect the opinions and feelings of others when discussing a topic in the major over the Internet	61	36	12	1	1
8	The importance of educating students and employees in cybersecurity	59	30	17	2	2
9	I need a specialized course in cybersecurity	63	23	18	4	3
10	Work to avoid information that is contrary to religion and belief	85	19	6	1	0
11	Respect the regulations of the Republic of Yemen in dealing with the Internet	66	26	10	8	1
12	Respect the policies of the websites that I use	66	29	9	6	1
13	Spread digital awareness when I am exposed to a problem or negative situations on the Internet	58	28	15	7	3
14	Avoid bypassing the laws imposed by the government in the use of the Internet	63	27	10	9	2
15	Use content licensed by the author or publisher	56	26	17	10	2
16	I support the college's setting of a system that prevents access to websites that could harm your computer.	82	19	7	2	1
17	Update the protection program on my device periodically	65	34	8	3	1
18	I support the development of procedures and policies to maintain the cybersecurity of the College	55	33	17	6	0
19	I use encryption for my important files that I send through the Internet	60	28	12	9	2
20	I observe integrity in my digital identity when I use social networking sites	64	21	10	6	10

Table 3. Results

Question no	SMA	s.davition	Percent	T-test	s.direction	q. rank
1	3.93	1.29	78.56	7.57	A	10
2	4.33	1.04	86.67	13.53	AS	5
3	4.33	1.02	86.67	13.76	AS	16
4	4.25	1.10	85.05	12.01	A	6
5	4.68	0.75	93.69	23.66	AS	7
6	4.57	0.86	91.35	19.23	AS	17
7	4.40	0.79	87.93	18.64	AS	12
8	4.25	1.00	85.05	13.14	A	2
9	4.25	1.03	85.05	12.80	A	3
10	4.69	0.61	93.87	29.03	AS	11
11	4.33	0.98	86.67	14.41	AS	14
12	4.38	0.92	87.57	15.88	AS	4
13	4.18	1.06	83.60	11.70	A	8
14	4.26	1.04	85.23	12.76	A	9
15	4.12	1.08	82.34	10.85	A	18
16	4.61	0.76	92.25	22.22	AS	19
17	4.43	0.82	88.65	18.50	AS	13
18	4.23	0.90	84.68	14.39	A	15
19	4.22	1.05	84.32	12.23	A	20
20	4.11	1.30	82.16	8.96	A	1

A visual inspection of this table immediately reveals that 47% of participants (94 participants) have Bachelor. Further, 2% of participants (3 participants) are Diploma and 6% of participants (11 participants) are Master. Only 3% of participants (6 participants) self - reported to have a PhD as shown in Table 1. Although there is no conclusive evidence that high education plays a role in mediating factors that affect cybersecurity awareness and behaviors, noted that experience has some effect on security self-efficacy. Further, it is noteworthy to highlight the experience composition of this sample.

3.2. Research Questions

To further investigate the cybersecurity awareness level of individuals in an academic setting, as stated in the research hypotheses; this study addresses the following research questions.

Table 2 shows the questionnaire output for all answers to the survey from the entire sample of participants (n=200) in this study.

3.3. A questionnaire results

The results presented in table 3 indicate a high degree of awareness among young people of cybersecurity concepts in general, and the responses of the sample members to the paragraphs of the first axis ranged from very pleading to pleading and neutral, as in table 3.

4. Conclusions

In recent years the concept of cybersecurity awareness has claimed the interest of researchers and academics in general. One of the main challenges in the study of cybersecurity is to better define the context in which this concept could be adopted and studied, regardless of changes in technology.

Awareness is frequently associated with operational situations, where specific reasons require individuals to have an identifiable awareness level for a specific context. Therefore, it is in the best interest of individuals and business organizations to seek out higher levels of cybersecurity awareness, since business continuity depends on how individuals respond to various situations, and ultimately, it depends on how well-informed individuals (users) are about current and future security risks in their doings. It's noted that individuals consider the internet to be a safe environment. However, their behavior does not reflect a high level of security awareness when

confronted with new cyber threats. Consequently, it is hard for organizations to plan for costs associated with cybersecurity incidents since tangible behaviors that depict awareness are not seen frequently.

The findings of this study can be considered beneficial in terms of adding up to the general body of knowledge in the field of cybersecurity awareness in Yemen. Further, several limitations prevent this study from generalizing results to make inferences about the population. Although there is no conclusive evidence that all demographic factors have an impact on the cybersecurity awareness level of individuals, it is noteworthy to mention that training 'Education Level' in one location seems to have an impact on the cybersecurity awareness level. Therefore, it would be necessary to further study more comprehensive groups of demographic factors to determine how relevant they are in the development of security awareness.

5. Future Research

Researchers would find it difficult to capture Yemenis studies in the field of cybersecurity awareness. Thus, future studies should take into consideration larger size of the sample. Moreover, the sample should include normal users and experienced users, professionals and academics and individuals and organizations. We advise to tackle gender comparisons and multiple demographics.

Conflicts of Interest

The authors declare no conflict of interest.

References

1 Ahmed N.; Islam M.R.; Kulsum U.; Islam M.R.; Haque M.E.; Rahman M.S. Demographic Factors of Cybersecurity Awareness in Bangladesh. In *2019 5th International Conference on Advances in Electrical Engineering (ICAEE),* 685-690. IEEE. [CrossRef]
2 Aljohani W.; Elfadil N. Measuring Cybersecurity Awareness of Students: A Case Study at Fahad Bin Sultan University. *Int. J. Comput. Sci. Mob. Computing*, 2020, **9**, 141-155. [Link]
3 Butler R.; Butler M. An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers. In *HAISA,* 2014 150-161. [Link]
4 Chandarman R.; Van Niekerk B. Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *Afr. J. Inf. Commun.*, 2017, **20**, 133-155. [CrossRef]
5 Elradi M.D.; Abd alraheem Altigani A.; Abaker O.I. Cyber Security Awareness among Students and Faculty Members in a Sudanese College. *Electrical Science & Engineering*, 2020, **2**. [CrossRef]
6 Garba A.A.; Siraj M.M.; Othman S.H. An Explanatory Review on Cybersecurity Capability Maturity Models. *Adv. Sci. Technol. Eng. Syst. J.*, 2020, **5**, 762-769. [Link]
7 Garba A.; Sirat M.B.; Hajar S.; Dauda I.B. Cyber Security Awareness among University Students: A Case Study. *Science Proceedings Series*, 2020, **2**, 82-86. [CrossRef]
8 Hariri R.; Amontashry F. The Degree of Awareness of Middle Female Teacher of Cybersecurity in Public Schools in Jeddah City from the Point of the Degree of Awareness of Middle Female Teacher of cs in Public Schools in Jeddah City from the Point of View of the Teachers. *The Arab Journal of Educational Quality*, 2020, **3**, 95-140.
9 Irfan H.; Akhter K.J.; Shakeel R. Cybersecurity and Multidisciplinary Students: A Survey. *Int. J. Sci. Eng. Res.*, 2020, **11**, 1786-1791. [Link]
10 Kim E.B. Recommendations for Information Security Awareness Training for College Students. *Information Management & Computer Security,* 2014. [CrossRef]
11 Peker Y.K.; Ray L.; Da Silva S.; Gibson N.; Lamberson C. Raising Cybersecurity Awareness among College Students. In *Journal of The Colloquium for Information Systems Security Education*, 2016, 4, 1-17. [Link]
12 Nagahawatta R.; Warren M.; Yeoh W. A Study of Cyber Security Issues in Sri Lanka. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 2020, **10**, 59-72. [CrossRef]
13 Pramod D.; Raman R. A Study on the User Perception and Awareness of Smartphone Security. *Int. J. Appl. Eng. Res.,* 2014, **9**, 19133-19144. [Link]
14 Tibi M.H.; Hadeje K.; Watted B. Cybercrime Awareness among Students at a Teacher Training College. *Int. J. Comput. Trends Technol.*, 2019, **67**, 11-17.